**REDACTED**

# UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

| | | |
|---|---|---|
| **In Re Search Of:** | ) | |
| **Information associated with the Gmail account:** | ) | **Case No. 2:17sw** 83 |
| **[redacted]@gmail.com that is stored at the premises** | ) | |
| **controlled by Google Inc.** | ) | |

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

**Information associated with the Gmail account: [redacted]@gmail.com that is stored at the premises controlled by Google Inc. located at 1600 Amphitheatre Parkway, Mountain View, California 94043. (As described in Attachment B)**

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

**See Attachment B-1.**

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section(s)* | *Offense Description* |
|---|---|
| 18 U.S.C. § 2252(a)(2) and (a)(4) | Transportation, distribution, receipt, and possession of child pornography |

The application is based on these facts: **See Affidavit.**

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:

_____
*Applicant's signature*

Paul G Wolpert, Special Agent (ICE) (HSI)
*Printed name and title*

_____
**Randy C. Stoker**
**Assistant United States Attorney**

Sworn to before me and signed in my presence.

Date: _____

_____
*Judge's signature*

City and state: _____

_____
*Printed name and title*

**REDACTED**

# AFFIDAVIT IN SUPPORT OF SEARCH WARRANT FOR E-MAIL ACCOUNTS

I, Paul G Wolpert, being first duly sworn state as follows:

## INTRODUCTION

1. I am a Special Agent of the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), currently assigned to the Office of the Assistant Special Agent in Charge (ASAC), Norfolk, Virginia. I have been so employed since April 2002. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)) in all forms of media including computer media. I make this application for a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure, and 18 U.S.C. § 2703(a) and (b), by which a court with jurisdiction over the offense may require the disclosure by a provider with electronic communication service of the contents of a wire or electronic communication. This affidavit seeks the issuance of a warrant for the disclosure of such contents of a iCloud and electronic mail accounts maintained by the electronic communications service providers known as "Apple", "Google Inc.", and "Juno".

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. This affidavit is being submitted in support of an application for a search warrant for the information and content associated with the following accounts ("the Accounts"):

a. Apple iCloud/iTunes account "[redacted]**@gmail.com**", used by **Robert Glaubke, Jr.,** and mobile number [redacted] from inception to present, that is or was stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company whose custodian of records is located at 1 Infinite Loop, Cupertino, CA, 95014, to include that information preserved by Apple, Inc. pursuant to the preservation request made on April 7, 2017, by Homeland Security Investigations pursuant to 18 U.S.C. 2703(f);

b. Google e-mail account **"[redacted]@gmail.com"** from inception to present, that is or was stored at the premises owned, maintained, controlled, or operated by Google Inc., a company whose custodian of records is located at 1600 Amphitheatre Parkway, Mountain View, California 94043; to include that information preserved by Google, Inc. pursuant to the preservation request made on April 7, 2017, by Homeland Security Investigations pursuant to 18 U.S.C. 2703(f);

c. Juno e-mail account "[redacted]**@juno.com**" from inception to present, that is or was stored at the premises owned, maintained, controlled, or operated by Juno Online Service, a company whose custodian of records is located at 2 Executive Drive, Suite 820, Fort Lee, NJ, 07024; to include that information preserved by Juno pursuant to the preservation request made on April 7, 2017, by Homeland Security Investigations pursuant to 18 U.S.C. 2703(f).

3. This affidavit is made, in part, in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc, Google Inc., and Juno to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the accounts, including the contents of communications. The information to be searched is described in the following paragraphs and in Attachments A, B, C, A-1, B-1, C-1.

4. This affidavit is based upon information that I have gained from my investigation, my training and experience, as well as information obtained from other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities (described in Attachments A, B, C, A-1, B-1, C-1) of violations of Title 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B) are within the information associated with the e-mail and other accounts mentioned above.

## LEGAL AUTHORITY

A. Pertinent Criminal Statutes

5. 18 U.S.C. § 2252(a)(2) provides that any person who knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct, shall be punished. 18 U.S.C. § 2252A(a)(2)(A) makes it a federal criminal offense to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

6. 18 U.S.C. § 2252(a)(4) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed, shipped or transported, by any means including by computer;

Title 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

B. Other Legal Authority

7. The legal authority for this search warrant application regarding the Accounts is derived from 18 U.S.C. §§ 2701-2711, entitled "Stored Wire and Electronic Communications and Transactional Records Access." Section 2703(a) provides in relevant part as follows:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

8. Section 2703(b) provides in relevant part as follows:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –
>
> > (A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.
>
> (2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –
>
> > (A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
> >
> > (B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

9. The government may also obtain records relating to e-mail communications, such as subscriber identifying information, by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A).

10. 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A) allow for nationwide service of process of search warrants for the contents of electronic communications and records concerning electronic communication service or remote computing service if such warrant is issued by a court with jurisdiction over the offense under investigation.

11. This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia, as more fully articulated below. *See* 18 U.S.C. § 3237(a); see also 18 U.S.C. §§ 3231 and 3232. *See United States v. Bagnell*, 679 F.2d 826, 830 (11th Cir. 1982) (venue is proper in child pornography and obscenity prosecution in district where images were either distributed or received).

## DEFINITIONS

12. The terms "records," "documents," and "materials" include all information recorded in any form, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

a. graphic records or representations;
b. photographs;
c. pictures;
d. images, and
e. aural records or representations.

13. The terms "records," "documents," and "materials" include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications may have been created or stored, including (but not limited to): any electrical, electronic, or magnetic form (including but not limited to any information on an electronic or magnetic storage device such as hard disks).

14. The terms "minor" and "sexually explicit conduct" are defined in 18 U.S.C. Section 2256(1) and (2). A "minor" is defined as "any person under the age of eighteen years." The term "sexually explicit conduct" means actual or simulated:

a. Sexual intercourse, including genital genital, oral genital, anal genital, or oral anal, whether between persons of the same or opposite sex;
b. Bestiality;
c. Masturbation;
d. Sadistic or masochistic abuse; or
e. Lascivious exhibition of the genitals or pubic area of any person.

15. The term "computer" as used herein is defined pursuant to Title 18 U.S.C. Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data

processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

16. The term "Universal Resource Locator" (URL): A URL is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

17. The term "Internet Protocol Address" (IP Address): This term refers to the fact that every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. There are two types of IP addresses; static and dynamic. A static address is permanent and never changes, such as ones used in cable modems. The dynamic address changes almost every time the computer connects to the Internet.

18. The term "Internet Service Provider" (ISPs): This term refers to individuals who have an Internet account and an Internet-based electronic mail (e-mail) address must have a subscription, membership, or affiliation with an organization or commercial service which provides access to the Internet. A provider of Internet access and services is referred to as an Internet Service Provider or "ISP".

19. "Web hosts" provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a Website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co location facilities offer customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

20. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. Title 18 U.S.C. Section 2510(15).

21. "Remote Computing Service" is a service that provides to the public computer storage or processing services by means of an "electronic communications system." Title 18 U.S.C. Section 2711.

22. "Electronic Communications System" means any wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Title 18 U.S.C. Section 2510(14).

23. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. Title 18 U.S.C. Section 2510(8).

24. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. Title 18 U.S.C. Section 2510(17).

## TECHNICAL BACKGROUND

25. E-mail is an electronic form of communication which usually contains written correspondence and graphic images. It is similar to conventional paper mail in that it is addressed from one individual to another and is usually considered private. An e-mail usually contains a message "header" which generally displays the sender's e-mail address, the recipient's e-mail address, and the date and time of the e-mail transmission.

26. If a sender chooses to do so, he or she can type a subject line into the header. E-mail message "headers" usually contain information, such as identification of the sender's ISP, which enables law enforcement officers to trace the message back to the original sender. In order to do so, information must be obtained from the sender's ISP through a Grand Jury or administrative subpoena.

27. Apple along with Google and Juno, are among other things, U.S.-based Internet Service Providers or "Web Hosts." The companies provide a full range of services including but not limited to: web based e-mail accounts, search engines, directories, travel resources, commercial services, and advertising. The company provides individuals with free web based e-mail accounts and services.

28. iCloud is Apple's cloud service that allows customers to access music, photos, applications, contacts, calendars, and documents from their iOS devices and Mac or Windows personal computers. It also enables customers to back up their iOS devices to iCloud, which as a result, information and data from the customer's iOS device is stored by Apple off the device. With the iCloud service, customers can utilize their own email account to set up the account. In some instances, the iOS device backup data may be the only known or existing source of the data.

29. An iPhone is an Apple device that uses the Apple iOS operating system. Additionally, an iPhone or other iOS device doesn't have to be registered with Apple, iTunes, or

iCloud in order to function; although it is common for iPhone users to register their iPhone with Apple in order to use the iPhone's vast features.

30. ITunes is a free Apple software application, which customers use to organize and play digital music and videos on their computers and devices as well as the marketplace to purchase "Apps" to be used on mobile devices.

31. In my training and experience, I have learned that the companies provide a variety of on-line services, including e-mail access, to the general public. Subscribers obtain an account by registering with the company. During the registration process, the company asks subscribers to provide basic personal information. Therefore, the computers of the company are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for the company's subscribers) and information concerning subscribers and their use of the company's services, such as account access information, e-mail transaction information, and account application information.

32. In general, an e-mail that is sent to the company's subscribers is stored in the subscriber's "mail box" on the company's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on the company's servers indefinitely.

33. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to the company's servers, and then transmitted to its end destination. The company often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the company's servers, the e-mail can remain on the system indefinitely.

34. The company's subscribers can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by the company.

35. Subscribers to the company might not store on their home computers copies of the e-mails stored in their account. This is particularly true when they access their account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

36. In general, e-mail providers like the company ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

37. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the company's websites), and other log files that reflect usage of the account. In addition, e-

mail providers often have records of the Internet Protocol address (IP address) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

38. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

39. In my training and experience, evidence of who was using an e-mail account and Instant Messenger accounts may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

## SUPPORTING FACTS

40. In February 2017 and other occasions, a detective with the Virginia Beach Police Department, Internet Crimes Against Children (ICAC) office was monitoring a peer-to-peer (P2P) file sharing network in an undercover capacity and was able to identify an IP address of [redacted] which was providing files of interest known to contain child pornography for distribution. On several occasions, the undercover detective successfully downloaded child pornography from the IP address.

41. Also between November 2016 and February 2017, an agent with the FBI Innocent Images Task Force was also monitoring the same Peer to Peer (P2P) file sharing network in an undercover capacity and identified the IP address of [redacted] which was providing files of interest known to contain child pornography for distribution. On several occasions the undercover agent successfully downloaded child pornography from the IP address.

42. The downloaded files and documentation from the Virginia Beach detective and FBI agent were turned over to your affiant for follow up investigation.

43. In addition to the previously received information, in January 2015 the HSI Cyber Crimes Center was investigating a website that had been identified providing child pornography as well as adult pornography. A review of the website access logs revealed numerous IP addresses that accessed the website and at least some of the child pornographic images. One such IP address was [redacted] which accessed the website on August 19, 2014. In February 2015, a customs summons was issued to Cox Communications for the account assigned the IP address [redacted] on August 19, 2014. The response from Cox revealed the account resolved to:

[redacted]
Norfolk, Virginia, [redacted]

In an effort to refresh the investigation several additional customs summonses were issued in late 2016 to February 2017 to determine the current assigned IP address for the residence, the most current response came on March 2, 2017. The responses repeatedly indicated the residence was assigned the IP address [redacted] and it had been assigned since June 17, 2015.

44. According to the activity logs, in all the instances of activity between the file sharing downloads and website access, the device that was used was an Apple device.

45. On April 4, 2017, agents and task force agents from HSI Norfolk, and the FBI, executed a search warrant at the residence at [redacted], Norfolk, VA, [redacted]. Present were Robert Glaubke [redacted] and [redacted]. Entry was made and the residence was secured. During the search, both occupants were interviewed and denied any knowledge of the identified activity. It was also learned their son, Robert Glaubke, Jr., did not reside there daily but often stayed there one to two nights a week when he was off work so he could visit his fiancé. Robert Glaubke, Jr., lives in Surry County. Both Mr. and Mrs. Glaubke stated their son used an iPhone. During the search of the residence the only Apple device that was located was an old iPad in the parents' room. During the search, [redacted] notified her son via text messaging that HSI was at the residence looking for child pornography and had asked about him. In a response, Glaubke, Jr., stated, he did not know why because he did not have a computer. Your affiant made contact with Glaubke, Jr., and arranged to meet. During the initial conversation, Glaubke, Jr., asked your affiant if he needed to bring his phone, in which your affiant responded he could if he wanted to, but I just wanted to talk to him about why we were at his parents' house.

46. Your affiant and a Chesapeake Police Detective (CPD) traveled to the pre-established meeting area and met with Glaubke, Jr. The agents identified themselves and sat in the CPD vehicle. Glaubke was advised no one was under arrest, and he could stop talking and leave at any time. Glaubke stated he understood. Your affiant asked Glaubke why he thought the agents had the information they did to execute a search at his parents' house and what kind of computers he used. Glaubke stated he did not know why child pornography was coming there. Glaubke also stated he did not have a personal computer, but had a laptop for work, and only used his iPhone to access the Internet. Glaubke stated he only used the Internet for Facebook and Instagram, and when pressed a little further denied even viewing adult pornography. After a few more minutes Glaubke asked if he could go use the restroom in which your affiant said of course. Prior to Glaubke leaving, your affiant asked him if he would allow the agents to verify that there was no child pornography on his phone. Glaubke agreed and handed your affiant his iPhone 7, [redacted], which is owned and operated by Verizon Wireless.

47. While accessing the phone, your affiant went to the Safari web browser and observed that all the recently viewed pages had been deleted. Next, your affiant went to the "History" bookmark which archives previously visited webpages and observed numerous website visits to a known pornography website named "Motherless.com". The website is known to provide images and videos of adult and child pornography that are posted by other users. Your affiant briefly viewed the URL titles for accessed files and saw the terms "teen" and "boys". Your affiant did not attempt to access the actual webpage. Also viewed were links to Dropbox, and Juno Webmail. According to the logs, the Juno Webmail account had been accessed that morning and part or all of its contents had been deleted in the browser.

48. After returning to the car, your affiant asked Glaubke about the entries in the History tab. Glaubke appeared to get nervous and his hands began to shake and he asked if he could text his fiancé. Your affiant informed Glaubke that his fiancé was being interviewed at that time and again stated that his previous statement about not even looking at adult pornography wasn't correct. Glaubke asked for his phone back. Your affiant explained to Glaubke that he was not done looking through the Internet history. Glaubke stated he wanted it back and that your affiant did not have a warrant to look through it and attempted to grab it out of your affiant's hand. Your affiant explained to Glaubke that he would get a search warrant to access his phone if that's what he wanted before your affiant looked any further. After more discussion, Glaubke provided the access passcode for the phone.

49. The interview continued and it was explained to Glaubke that the investigators were only trying to determine the responsible party for the identified activity and further identify if the extent of the activity was entirely online or may have led to hands on activity. Glaubke was informed that his reaction and physical response was concerning to the agents if he had nothing to worry about. Glaubke listened to the agents and acknowledged their concerns. Glaubke was asked what he believed the youngest to be that he had seen while viewing pornography. Glaubke was also asked if he had seen "infants or toddlers", and if he knew the difference between a five and a twelve-year-old. In response to each question, Glaubke responded with "I don't know, I don't want to talk about it". After the third question, Glaubke stated he was getting upset and stated he didn't want to talk anymore until talking to an attorney. Glaubke exited the vehicle and was provided with contact information for the investigating agents.

50. On April 6, 2017, your affiant applied for and received a search warrant for the contents of Glaubke's cellphone. An examination was conducted of the available contents. The text message from his mother informing him that HSI was at his residence looking for child pornography was recovered. A review of the web browser activity showed minutes after receiving the text message Glaubke visited the web based email service Juno and accessed his Juno account of [redacted]**@juno.com** and deleted email from his inbox, and then accessed the trash folder. The browser history also showed Glaubke accessed a Gmail account at the same time. The user settings for the iPhone indicated Glaubke used the email account [redacted]**@gmail.com** to register for his iTunes and iCloud account. Preservation letters were sent to Apple, Gmail, and Juno to preserve the contents of the accounts on April 7, 2017.

51. After the execution of the search warrant on April 4, 2017, your affiant contacted Glaubke's fiancé and learned he had previously lived with another member of her family at a residence in Chesapeake, VA, and obtained the address. A summons was issued to their Internet provider for the IP address assigned during the period that Glaubke lived there.

52. Your affiant received the IP address and checked a law enforcement data base that logs child pornography activity over the peer to peer networks. The IP address was identified providing child pornography for distribution from a period between May to August 2016. According to the former roommate Glaubke moved out of the residence in September 2016.

53. Your affiant has also received and reviewed Glaubke's work schedule for the relevant time periods and discovered Glaubke was scheduled off when the activities related to child pornography occurred.

54. Your affiant obtained Court Orders to Verizon Wireless to provide cell site information for the location of Glaubke's cellphone during the relevant periods of activity for the downloads of child pornography. On or about May 6, 2017 and June 18, 2017 your affiant received the account information from Verizon Wireless and a review of the relevant dates indicated Glaubke was in the vicinity of his parents' residence during all the download activity and not in the area of Surry, VA where he resides. In addition the information also placed Glaubke's phone in the vicinity of his former residence in Chesapeake, VA, during the activity that was detected in July and August 2016.

## CONCLUSION

55. On the basis of the above described facts, I respectfully submit that there is probable cause to believe that the stated Apple, Gmail, and Juno email and iCloud accounts have been used with the distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), which prohibit the knowing receipt or distribution of visual depictions of and involving the use of a minor engaging in sexually explicit conduct in interstate or foreign commerce, and the knowing possession of or access with the intent to view one or more matters containing any visual depictions of and involving the use of a minor engaging in sexually explicit conduct that have traveled in interstate or foreign commerce or were produced using material so transported or shipped.

56. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities of such violations will be found within the information associated with the Apple, Gmail, and Juno email and iCloud accounts (more particularly described in Attachments A, B, C) for evidence of Activities Relating to Material Involving the Sexual Exploitation of Minors, in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B). Accordingly, I request that warrants be issued authorizing HSI agents, with assistance from other law enforcement personnel, to search those accounts, obtain the information in the accounts and to seize all contents referred to Attachments A-1, B-1, C-1.

Paul G Wolpert
Special Agent
Department of Homeland Security
Homeland Security Investigations

SUBSCRIBED and SWORN before me this ___ of June, 2017

_____
UNITED STATES MAGISTRATE JUDGE

## ATTACHMENT B

### DESCRIPTION OF THE PREMISES TO BE SEARCHED

This warrant applies to information associated with the Google Inc. account [redacted]**@gmail.com**, from inception to present, that is or was stored at the premises owned, maintained, controlled, or operated by Google Inc., a company whose custodian of records is located 1600 Amphitheatre Parkway, Mountain View, California 94043; to include that information preserved by Google, Inc. pursuant to the preservation request made on April 7, 2017, by Homeland Security Investigations pursuant to 18 U.S.C. 2703(f);

## ATTACHMENT B-1

## PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Google Inc.:

To the extent that the information described in Attachment B-1 is within the possession, custody, or control of Google Inc., Google Inc. is required to disclose the following information to the government for each account listed in Attachment B:

- The contents of all e-mails stored or that were stored in the account, including copies of e-mails sent from the account;
- All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- All records pertaining to communications between Google Inc. and any person regarding the account, including contacts with support services and records of actions taken;

II. Information to be seized by the government

All information described above in Section I and content that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252, and 2252A including, for each user ID identified on Attachment B, information pertaining to the following matters:

- content e-mail accounts [redacted]**@gmail.com**
- content pertaining to requesting images or pictures;
- the attempted or actual receipt, distribution and possession of child pornography; and
- records relating to who created, used, or communicated with the user accounts.